

AB:ADW

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- X

IN THE MATTER OF THE SEARCH OF THE  
PREMISES KNOWN AND DESCRIBED AS  
2072 77<sup>TH</sup> STREET, APARTMENT 5, BROOKLYN  
NEW YORK 11214 AND ANY CLOSED  
CONTAINERS/ITEMS CONTAINED THEREIN

**FILED UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF  
A SEARCH WARRANT**

----- X **19-MJ-1178**

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41  
FOR A WARRANT TO SEARCH AND SEIZE**

I, ELIZABETH JENSEN, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 2072 77<sup>TH</sup> STREET, APARTMENT 5, BROOKLYN NEW YORK 11214 (the “SUBJECT PREMISES”), further described here and in Attachment A, for the things described in Attachment B.

2. I have been a Special Agent of the FBI since January 2011, and am currently assigned to the New York Field Office. I have been assigned to a Crimes Against Children squad and investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous child pornography cases and have reviewed thousands of photographs depicting children (less than eighteen years of age) being sexually

exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

3. The FBI is investigating the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

4. Based on the following paragraphs, I submit that there is probable cause to believe that there is kept and concealed within the SUBJECT PREMISES, the items described in Attachment A to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

5. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant, and does not set forth all of my knowledge about this matter.

**THE SUBJECT PREMISES**

7. The SUBJECT PREMISES is an apartment within a residential building located at 2071 77th Street in Brooklyn, New York. The building has a brick exterior. The numbers “2072” are affixed to the front of the building. The apartment building has a main entrance that proceeds to a long hallway. The SUBJECT PREMISES is on the third floor of the building, facing 77th Street. The door to the SUBJECT PREMISES is green with a gold colored peep hole and door handle. There is a hallway mat outside the SUBJECT PREMISES.



8. On or about December 6, 2019, FBI agents, using a ruse, went to the SUBJECT PREMISES and spoke to a female individual “TATYANA,” who stated the SUBJECT PREMISES was “APARTMENT 5” and was the “UZUNOV RESIDENCE.”

9. Based on my investigation to date, I believe that in addition to the female identified as “TATYANA,” there are two male occupants living in the SUBJECT PREMISES: Krastiou Uzunov and Toncho Uzunov.

10. A search of records maintained by Con Edison, a public utilities provider to the greater New York City area, shows that an individual by the name of “KRASTIOU UZUNOV” receives utilities at the SUBJECT PREMISES.

11. Upon information or belief, there are no minors living at the SUBJECT PREMISES.

### **DEFINITIONS AND BACKGROUND**

12. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

- a. The terms “minor,” “sexually explicit conduct,” and “visual depiction” are defined as set forth in Title 18, United States Code, Section 2256.
- b. The term “child pornography” is defined in Title 18, United States Code, Section 2256(8), in pertinent part, as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . .”<sup>1</sup>
- c. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets,

---

<sup>1</sup> See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

- d. The term “IP Address” or “Internet Protocol Address” means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.
- e. The term “Internet” refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- f. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.
- g. The term “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

13. Peer to Peer (“P2P”) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be

downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others who are running compatible P2P software. BitTorrent is one type of P2P software, which sets up its searches by keywords, typically on torrent websites. BitTorrent programs are typically free to download and are used for the exchange of files between computer users.

14. A user can use this software to perform a keyword search over the Internet. The results of a keyword search are displayed to the user via a website. The website itself does not contain the actual files intended to be shared, but instead provides a “torrent” file. A torrent is a small file that describes the files to be shared and provides details allowing the user to identify which of the available files he or she may wish to access. The user then selects which torrent file(s) from among the results to download. This torrent file contains download instructions for the user to download the file(s) referenced in the torrent that he/she wishes to access. The file can be downloaded through a direct connection between the computer requesting the file(s) and the computer(s) sharing the file(s). For example, a person interested in obtaining child pornography images could open the BitTorrent website on his/her computer and conduct a keyword search for files using a term such as “preteen sex.” The results of the search would then be returned to the user’s computer and displayed on the torrent site. The user then selects a torrent from among the results displayed corresponding to the file(s) he/she wants to download. Once the torrent file is downloaded, a previously-installed BitTorrent program is used to access the file content. The torrent file provides the set of instructions that the BitTorrent program needs to find the files identified in the torrent file. The file(s) are then downloaded directly

from the sharing computer(s). The downloaded file(s) are stored in an area designated by the user and/or the software. The downloaded file(s) will remain in that location until moved or deleted.

15. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers. This speeds up the time it takes to download the file.

16. A P2P file transfer is assisted by reference to an IP address. This address is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers. The computer running the file sharing application, in this case a BitTorrent application, has an IP address assigned to it while it is connected to the Internet.

17. BitTorrent users are able to see the IP address of any computer system sharing files with them or receiving files from them. When investigating subjects who share or access child pornography via P2P applications, investigators log the IP address that has sent them files or information regarding files being shared. Investigators can then search public records that are available on the Internet to determine the Internet Service Provider (ISP) who has assigned that IP address.

18. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the Internet Service Provider.<sup>2</sup>

19. An IP address is associated with a modem that is connected to the Internet. The IP address does not identify the specific computer or electronic device that is connected to the Internet. The IP address also cannot identify how many computers or electronic devices are connected to a router by a subscriber or at a subscriber's location. Through the use a of router, which is connected to the modem, multiple electronic devices including laptops, cell phones, desktop computers, televisions could be connected to the Internet and share the same IP address.

#### **PROBABLE CAUSE**

20. Law enforcement observed a BitTorrent network user sharing child pornography from the IP address 24.191.123.28 on October 8, 2019. Between October 8, 2019 and October 9, 2019, an FBI Special Agent working in an undercover capacity (the "Undercover Agent"), used a BitTorrent application via an Internet-connected computer located within the FBI's New York Division to conduct undercover investigations into the Internet distribution and possession of child pornography. During this time period, law enforcement officers observed a computer assigned the IP address 24.191.123.28 sharing child pornography on the BitTorrent file sharing network on at least two separate occasions. The sharing computer's IP address was recorded along with the date and time of the file

---

<sup>2</sup> In my experience, a residential premises generally has one Internet Service Provider, and thus, one IP address for all of the computers and electronic devices that connect to the Internet from within the premises.



transfer. The sharing computer reported that it was using BitTorrent client software “uTorrent 3.3.”

21. When users on BitTorrent download files, the computers sharing files on BitTorrent can be identified by their IP addresses. The IP address assigned to the computer sharing the above files on BitTorrent during the abovementioned time period was 24.191.123.28.

22. During the abovementioned time period, the Undercover Agent downloaded over 7000 video files and/or images containing child pornography. All of these files were downloaded from the sharing computer assigned to the IP address 24.191.123.28.

23. I have reviewed the files downloaded by the Undercover Agent from the IP address 24.191.123.28. Several of these files, which are available for the Court’s review, are described as follows:

- a. **baby girl riding dads dicks 2.jpg** is an image of an adult male inserting his penis into the vagina of a prepubescent girl, approximately three to five years old.
- b. **baby&dick6** is an image of an adult males’ penis at the mouth of a baby, approximately three to eight months old.
- c. **[clip][toddler]-girl-babykim-april05(licking\_her\_cunt,taste\_her\_piss,rubbing\_my\_cock).avi** is a video of a prepubescent girl, approximately six to eighteen months old, and an adult male’s penis is rubbing her vagina. The adult male’s tongue then licks the same girl’s vagina until she urinates.

24. Open source database searches of the IP address 24.191.123.28 identified Optimum as the ISP.

25. Based on records obtained from Optimum by administrative subpoena, the IP address 24.191.123.28 was identified as belonging to the SUBJECT PREMISES and to subscriber “ARASTIOU UGUNOV” (sic).

26. The IP address 24.191.123.28 is associated with a router located at the SUBJECT PREMISES that is connected to the Internet. Through the use of a router, which is connected to the modem, multiple electronic devices including laptops, cell phones, desktop computers, televisions, located within the SUBJECT PREMISES could be connected to the Internet and use the IP address 24.191.123.28. Thus, any computer or electronic device within the SUBJECT PREMISES could contain evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A.

#### **CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY**

27. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

28. I know that collectors of child pornography often retain their materials and related information for many years.

29. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

30. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

31. Based on my experience, I know that persons who collect and distribute child pornography often collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

32. In addition, based on my training and experience, I know that persons who collect and distribute child pornography very frequently use cell phones and other mobile electronic devices to possess, trade, and/or produce child pornography, and to communicate with minors. Based on my experience in investigating child pornography crimes, I have seen users possess, distribute and receive child pornography through cell phone applications, including BitTorrent, which can be installed on a mobile electronic device.

33. In addition, based on my training, experience, and investigations into child pornography crimes, I have also seen collectors of child pornography store, possess, distribute and receive child pornography in various areas of a premise, including in concealed areas in common spaces and on computers and electronic storage devices that can

be used or accessed by others. For example, a single computer can be used by more than one user, through different login accounts and/or account profiles, and based on my experience in investigating child pornography crimes, a collector of child pornography could store and view child pornography on that computer through his/her unique account profile. Until a given electronic device has been examined, there is no way to determine whether it was used to facilitate the criminal conduct under investigation or whether items relevant to the investigation have been transferred to such device.

34. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions, officers have recovered evidence related to the production of child pornography and/or child exploitation.

### **TECHNICAL BACKGROUND**

35. As described above and in Attachment B, this application seeks permission to search for records that constitute evidence, fruits or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A that might be found in the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

36. I submit that if a computer or electronic storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space — that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media — in particular, the internal hard drives of computers — contain electronic evidence of how a computer has been used, what it has been used for,

and who has used it. For example, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

37. Based on the evidence that at least one computer or electronic device connected to a P2P network through an IP address registered at the SUBJECT PREMISES, there is reason to believe that there is at least one computer or electronic device currently located on the SUBJECT PREMISES.

38. In addition, as further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic “attribution” evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of

a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

39. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. This is true because of the time required



for examination, technical requirements, and the variety of forms of electronic media, as explained below:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the SUBJECT PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

40. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would authorize seizing, imaging, or otherwise copying computers and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

41. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. Law enforcement personnel will seize computers, cellular devices or electronic storage media that law enforcement personnel reasonably believe—based on the location of such devices within the SUBJECT PREMISES, any identifying information on the exterior of such devices, and any other information about such devices available to law enforcement personnel—that either are or have previously been used by, whether directly or indirectly, one or more individuals who are suspected to have committed the SUBJECT OFFENSES or that may otherwise contain any electronically stored information falling within the categories set forth in Attachment B.

**CONCLUSION**

42. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT PREMISES described in Attachment A and seize the items described in Attachment B.

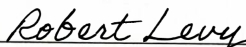
**REQUEST FOR SEALING**

43. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation at the SUBJECT PREMISES to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.



Special Agent Elizabeth Jensen  
Federal Bureau of Investigation

Sworn to before me this  
17th day of December, 2019



THE HONORABLE ROBERT M. LEVY  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A**  
Property to Be Searched

SUBJECT PREMISES is an apartment within a residential building located at 2071 77th Street in Brooklyn, New York. The building has a brick exterior. The numbers “2072” are affixed to the front of the building. The apartment building has a main entrance that proceeds to a long hallway. The SUBJECT PREMISES is on the third floor of the building, facing 77th Street. The door to the SUBJECT PREMISES is green with a gold colored peep hole and door handle. There is a hallway mat outside the SUBJECT PREMISES.



**ATTACHMENT B**  
**Property to Be Seized**

Items to be seized from the SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A (the “SUBJECT OFFENSES”) from January 1, 2018 through the present:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;
2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:
  - a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
  - b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.
7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
8. Records evidencing occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.
9. Records or other items which evidence ownership or use of computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.
10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.
11. Address books, names, lists of names and addresses of individuals believed to be minors.
12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.
13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.
14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers<sup>1</sup> or storage media<sup>2</sup> that contain records or information (hereinafter “COMPUTER”) used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;
  - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
  - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
  - f. evidence of the times the COMPUTER was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

---

<sup>1</sup> A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

<sup>2</sup> A “storage medium” for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - i. contextual information necessary to understand the evidence described in this attachment;
- 16. Records and things evidencing the use of the Internet Protocol address 184.152.164.88, including:
  - a. routers, modems, and network equipment used to connect computers to the Internet;
  - b. Internet Protocol addresses used by the COMPUTER;
  - c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- 17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.
- 18. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. Law enforcement personnel will seize computers, cellular devices or electronic storage media that law enforcement personnel reasonably believe—based on the location of such devices within the SUBJECT PREMISES, any identifying information on the exterior of such devices, and any other information about such devices available to law enforcement personnel—that either are or have previously been used by, whether directly or indirectly, one or more individuals who are suspected to have committed the SUBJECT OFFENSES or that may otherwise contain any electronically stored information falling within the categories set forth in Attachment B.